Web Gateway Cloud Service IPSec Configuration

Juniper SSG5 Example - NetScreen 6.3.0r21.0 (Firewall+VPN)

This document describes configuration of the Juniper SSG5 device running NetScreen OS. The tested NetScreen version was 6.3, but we expect the configuration to work with other versions and appliances running similar OS. Key capabilities are IPSec Gateway to Gateway VPN supporting IKEv2 and Policy Based routing for any destination (0.0.0.0/0).

All configuration assumes that the firewall is already set up for basic routing:

- Ethernet0/0 is configured in the Untrust zone, and bgroup0 is configured in the Trust zone.
- McAfee Web Gateway Cloud Service (McAfee WGCS) is configured with a pre-shared secret, your external public IP, and the local subnet where client web traffic is sourced.

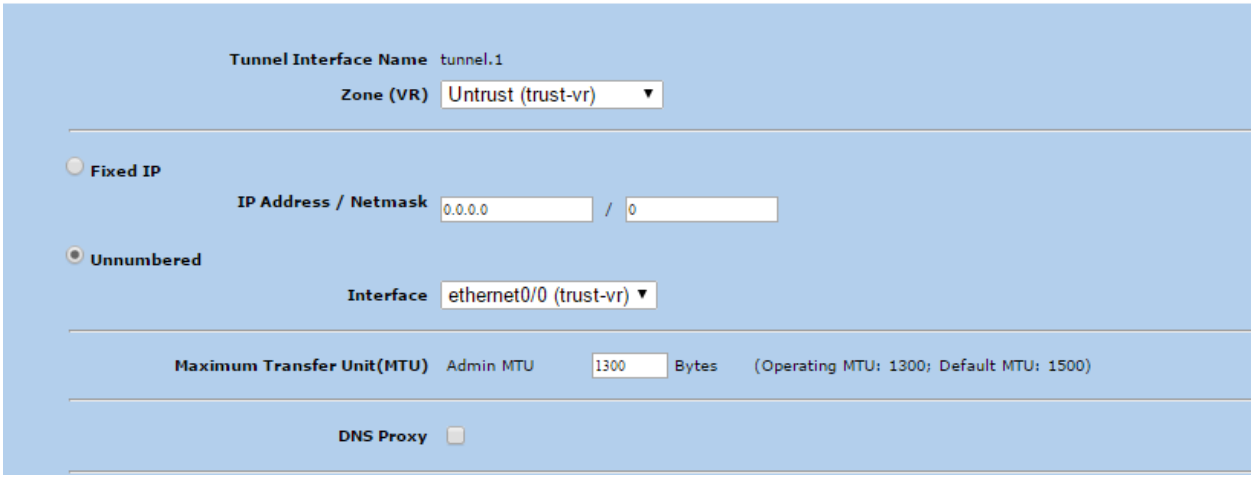
Basic Steps

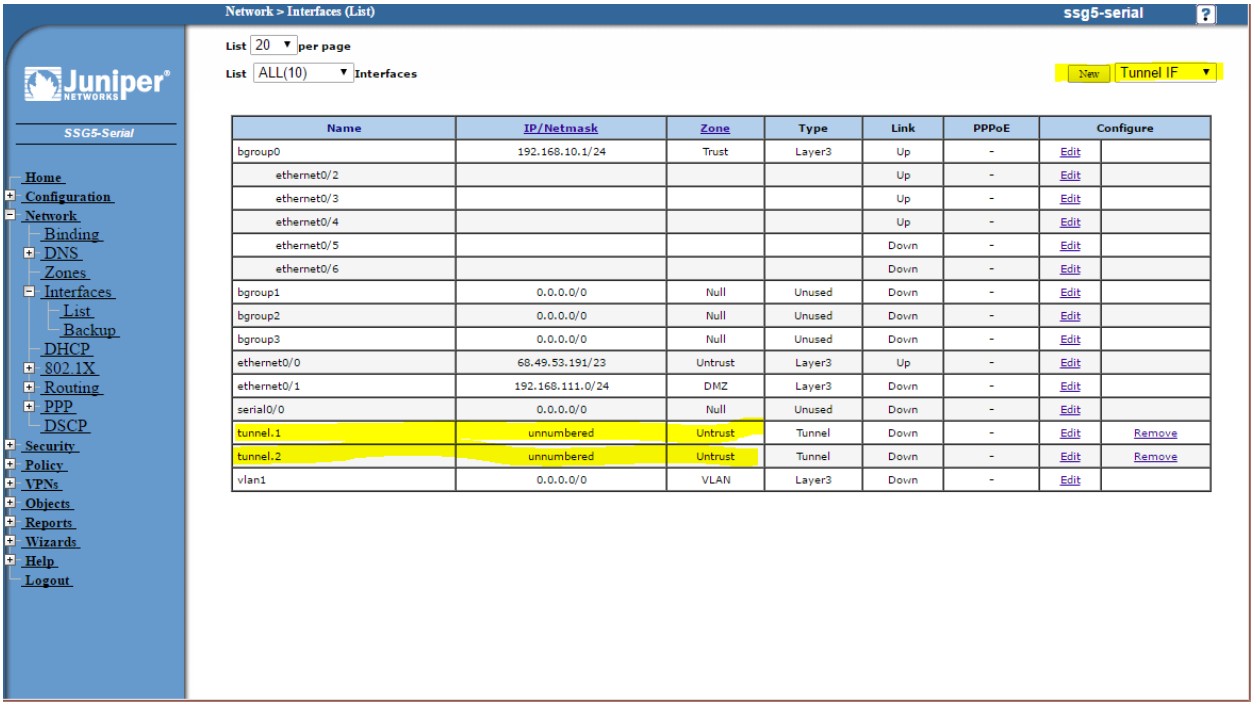
1. Configure Tunnel Interfaces
2. Configure VPNs and Bind to Tunnel Interfaces
3. Create Policy Based Routing (PBR) Policy
4. Bind PBR Policy to Client Interface(s)

Configure Tunnel Interfaces

From **Network > Interfaces > List**, add two new tunnel interfaces to the Untrust zone.

- **Zone (VR)** – Untrust (trust-vr)
- **Unnumbered** – Selected
- **Interface** – ethernet0/0 (trust-vr)
- **Maximum Transfer Unit(MTU)** – 1300



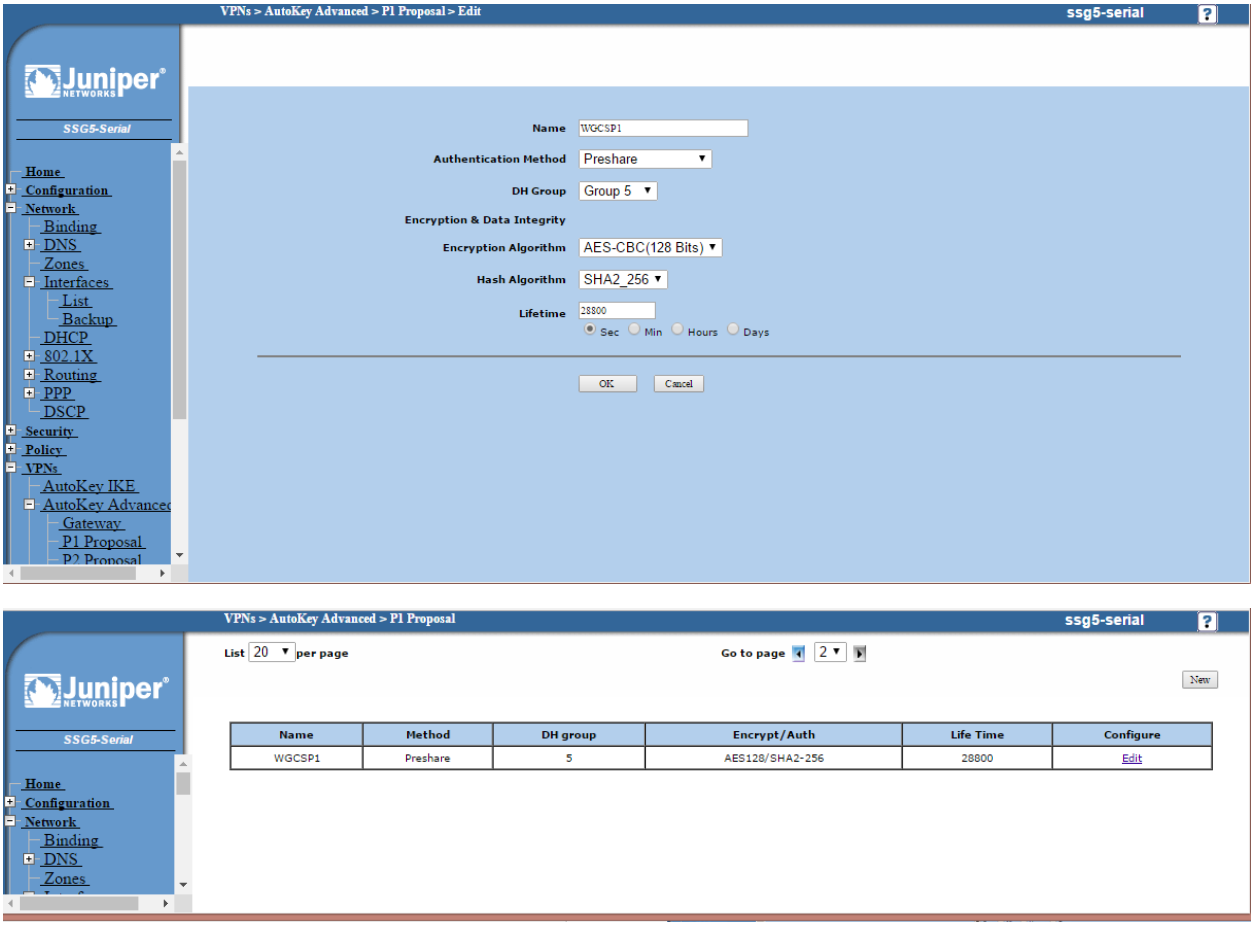


Name	IP/Netmask	Zone	Type	Link	PPPoE	Configure	
bgroup0	192.168.10.1/24	Trust	Layer3	Up	-	Edit	
ethernet0/2				Up	-	Edit	
ethernet0/3				Up	-	Edit	
ethernet0/4				Up	-	Edit	
ethernet0/5				Down	-	Edit	
ethernet0/6				Down	-	Edit	
bgroup1	0.0.0.0/0	Null	Unused	Down	-	Edit	
bgroup2	0.0.0.0/0	Null	Unused	Down	-	Edit	
bgroup3	0.0.0.0/0	Null	Unused	Down	-	Edit	
ethernet0/0	68.49.53.191/23	Untrust	Layer3	Up	-	Edit	
ethernet0/1	192.168.111.0/24	DMZ	Layer3	Down	-	Edit	
serial0/0	0.0.0.0/0	Null	Unused	Down	-	Edit	
tunnel.1	unnumbered	Untrust	Tunnel	Down	-	Edit	Remove
tunnel.2	unnumbered	Untrust	Tunnel	Down	-	Edit	Remove
vlan1	0.0.0.0/0	VLAN	Layer3	Down	-	Edit	

Configure VPNs and Bind to Tunnel Interfaces

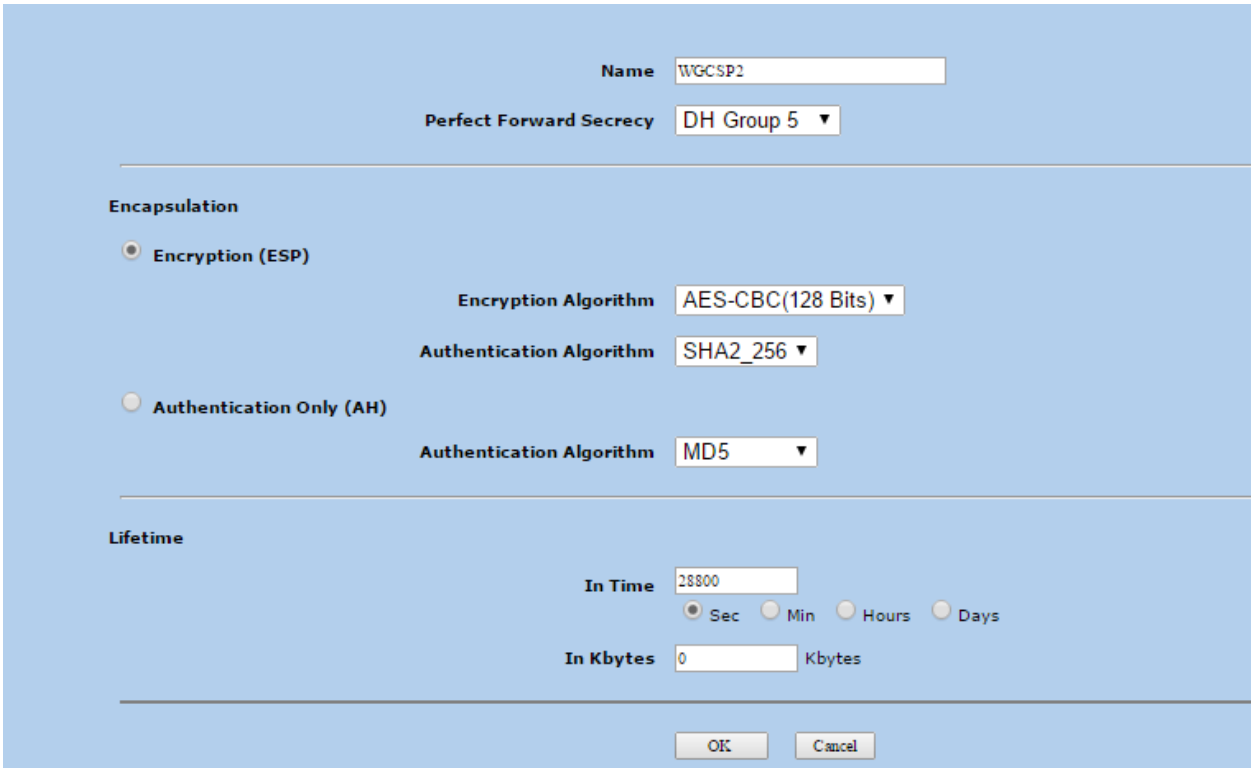
From **VPNs > AutoKey Advanced > P1 Proposal**, create a custom Phase One Proposal.

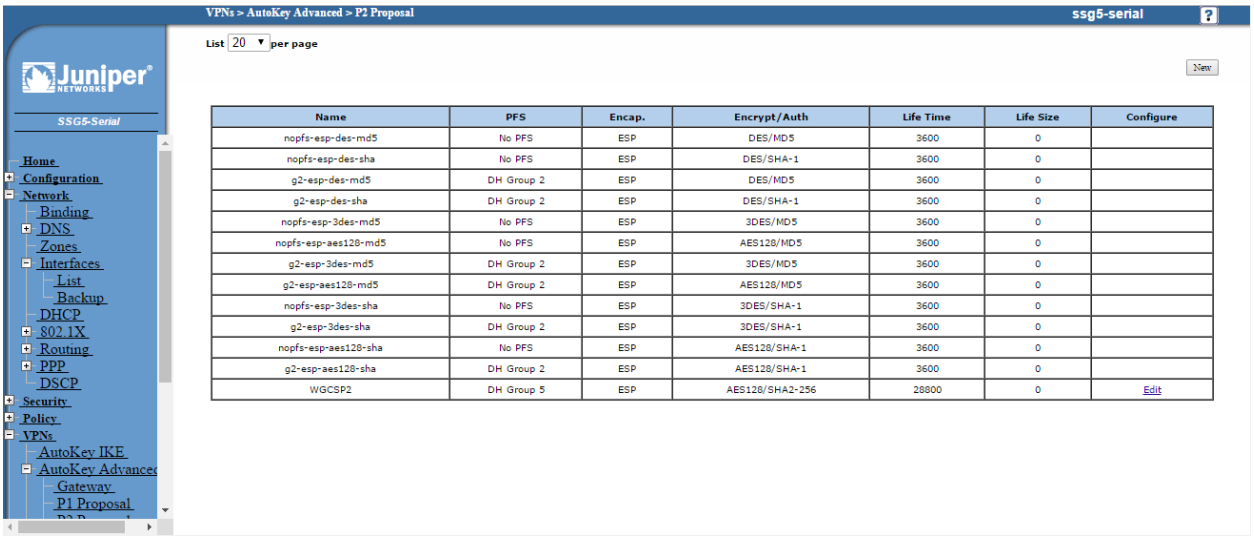
- **Name** – WGCSP1 (example)
- **Authentication Method** – Preshare
- **DH Group** – Group 5
- **Encryption Algorithm** – AES-CBC(128 Bits)
- **Hash Algorithm** – SHA2_256
- **Lifetime** – 28800 (Sec)



From **VPNs > AutoKey Advanced > P2 Proposal**, create a custom Phase Two Proposal.

- **Name** – WGCSP2 (example)
- **Perfect Forward Secrecy** – DH Group 5
- **Encryption (ESP)** – Selected
- **Encryption Algorithm** – AES-CBC(128 Bits)
- **Authentication Algorithm** – SHA2_256
- **Lifetime** – 28800 (Sec)



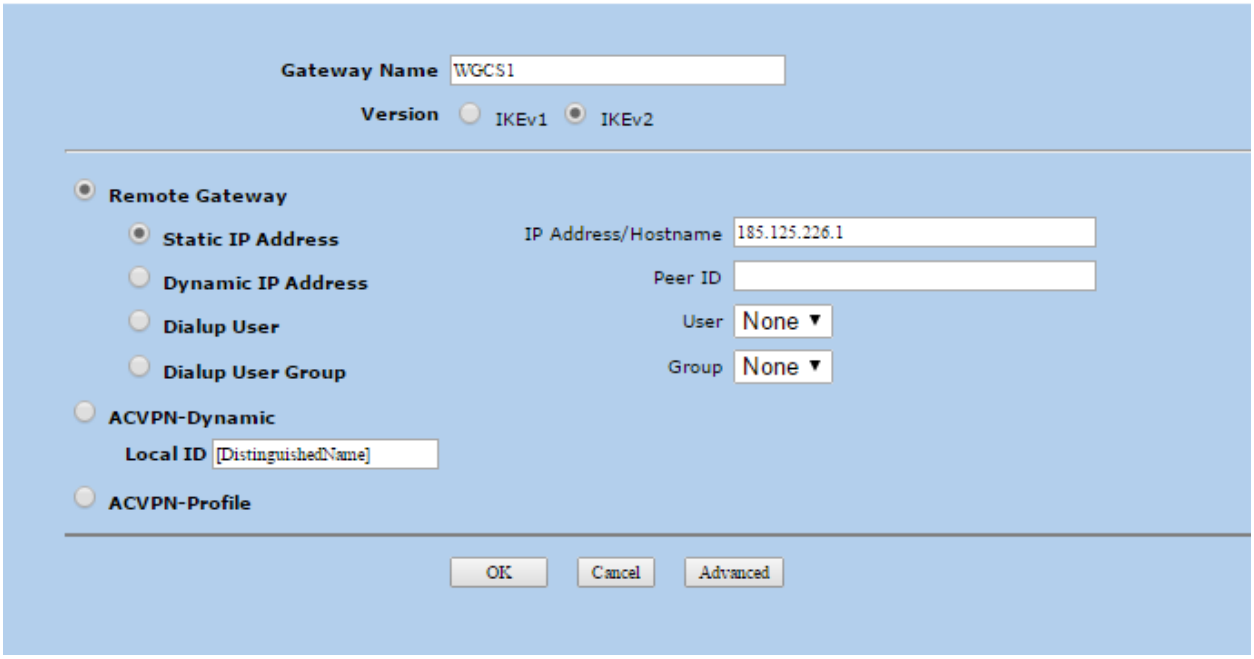


Create two VPN Gateway definitions – When you repeat this procedure for the second Gateway, assign a different name and static IP address.

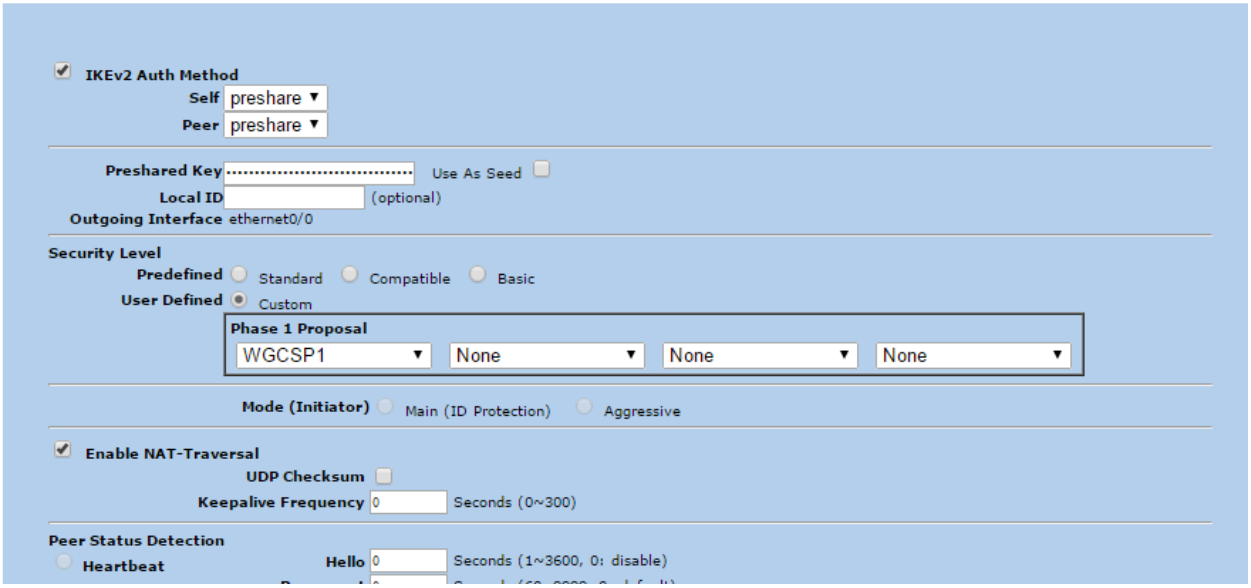
From **VPNs > AutoKey Advanced > Gateway**, configure these settings.

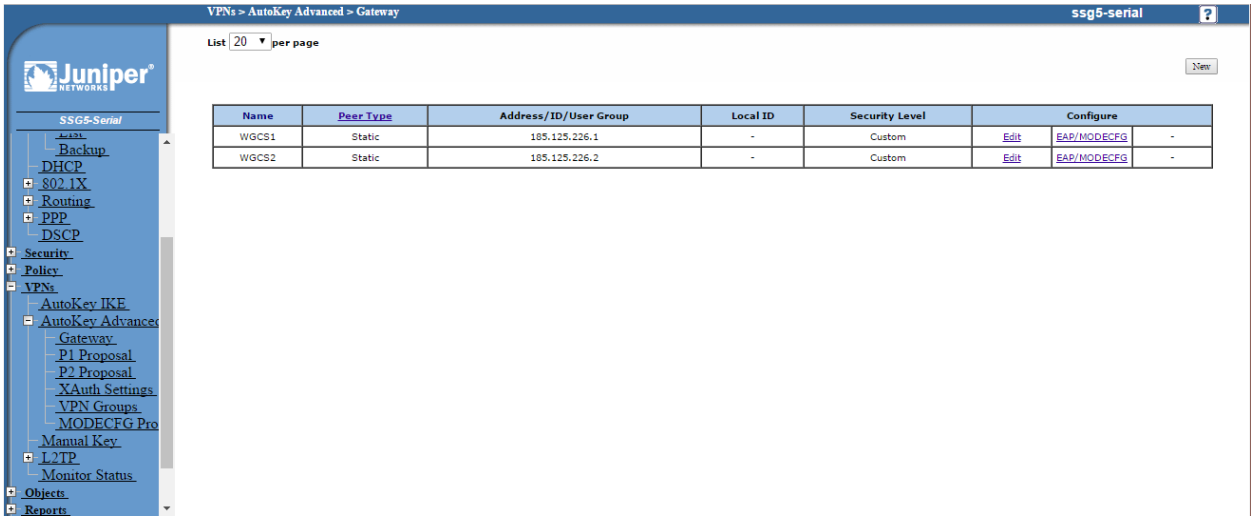
- **Gateway Name** – WGCS1 or WGCS2 (examples)
- **Version** – IKEv2
- **Remote Gateway** – Selected

- **Static IP Address** – Specify the resolved IP address for each gateway from a DNS lookup of 1.network.c<customerid>.saasprotection.com or 2.network.c<customerid>.saasprotection.com.
- **IKEv2 Auth Method** – Selected
- **Self** – preshare
- **Peer** – preshare
- **Preshared Key** – Must match the value configured in McAfee WGCS
- **Security Level** – Select **User Defined** (Custom).
- **Phase 1 Proposal** – Select WGCSP1, None, None, None.
- **Enable NAT-Traversal** – Selected



Click **Advanced** to open more settings.

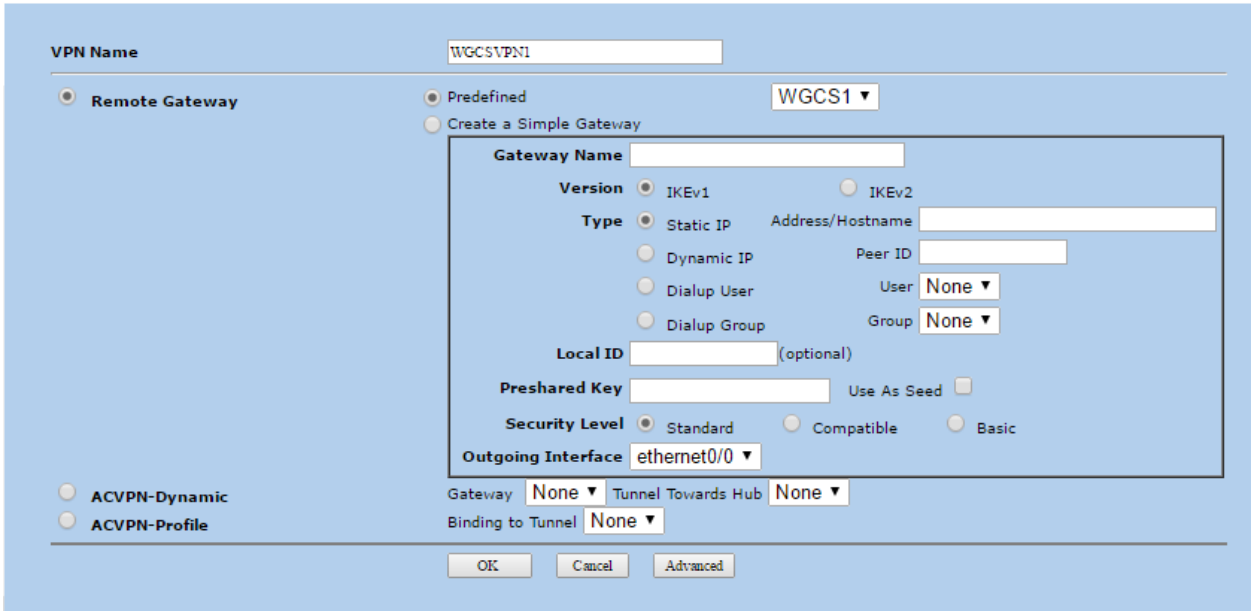




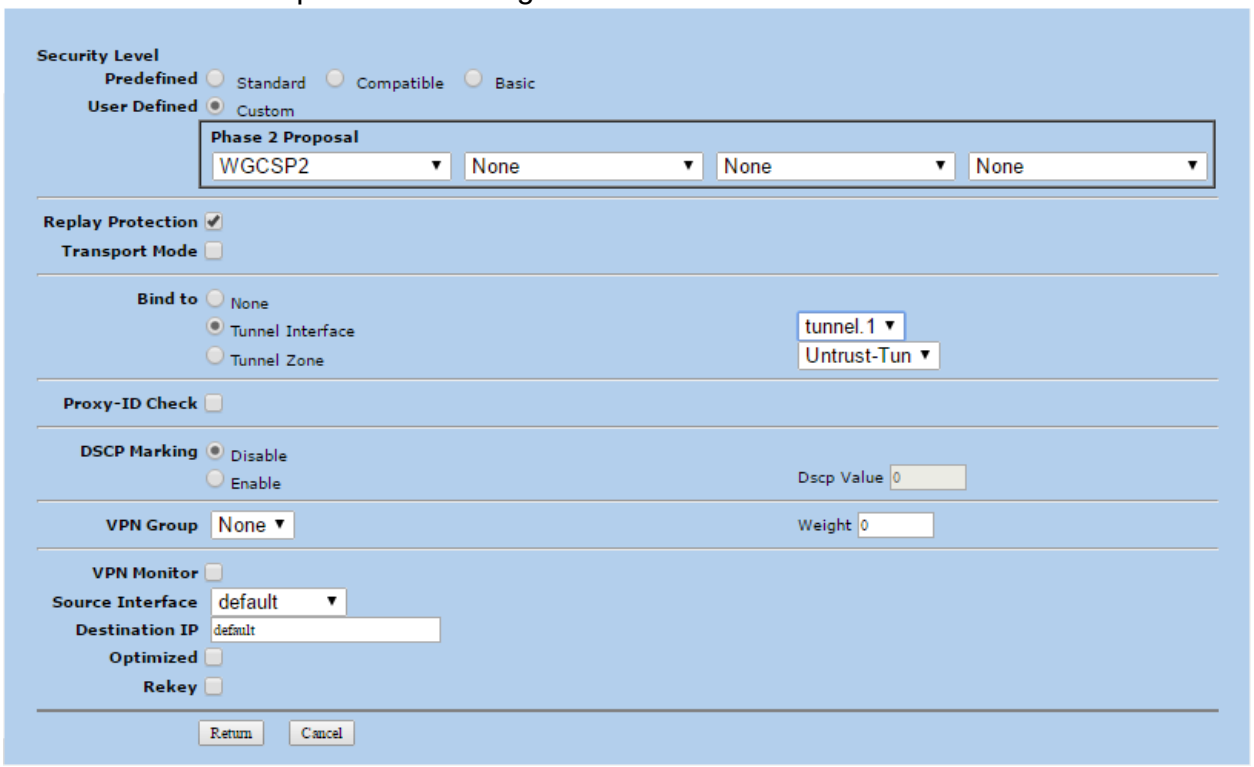
Create a VPN tunnel binding for two tunnel interfaces – When you repeat this procedure for the second interface (tunnel. 2), assign the VPN binding a different name, such as WGCSVPN2.

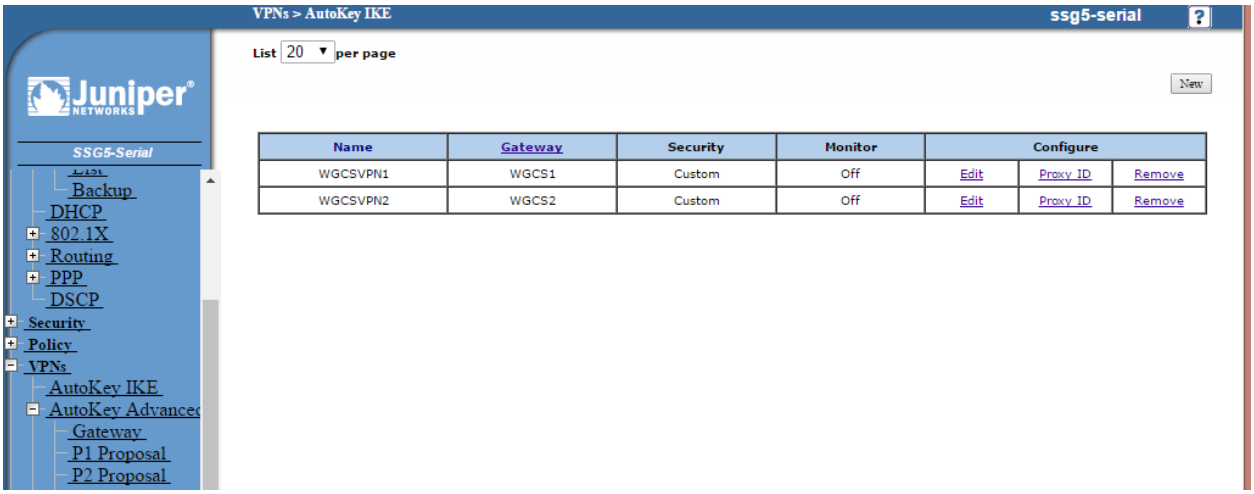
From **VPNs > AutoKey IKE**, configure these settings.

- **VPN Name** – WGCSVPN1 or WGCSVPN2 (examples)
- **Remote Gateway** – Selected
- **Predefined** – WGCS1
- **Security Level** – Select **User Defined** (Custom).
- **Phase 2 Proposal** – Select WGCSP2, None, None, None.
- **Bind to** – Select **Tunnel Interface**, tunnel.1.



Click **Advanced** to open more settings.



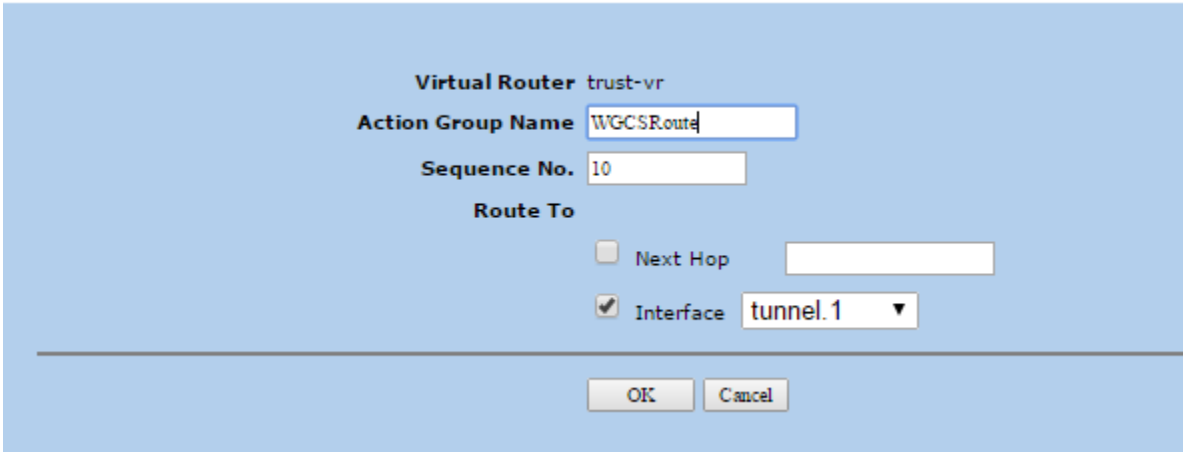


Create Policy Based Routing (PBR) Policy

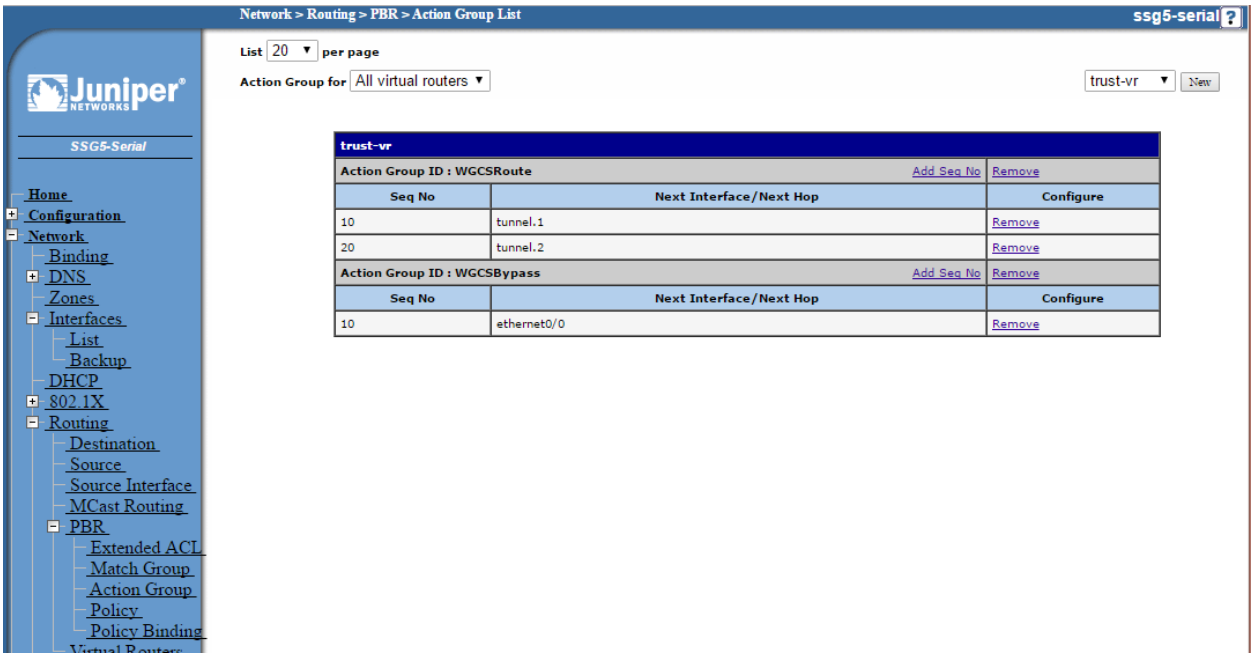
Create an Action Group with two routes – When you repeat this procedure for the second route, use 20 for the sequence number and tunnel.2 for the interface.

From **Network > Routing > PBR > Action Group**, configure these settings.

- **Virtual Router** – trust-vr
- **Action Group Name** – WGCSRoute (example)
- **Sequence No.** – 10
- **Route To** – Select **Interface**, tunnel.1.



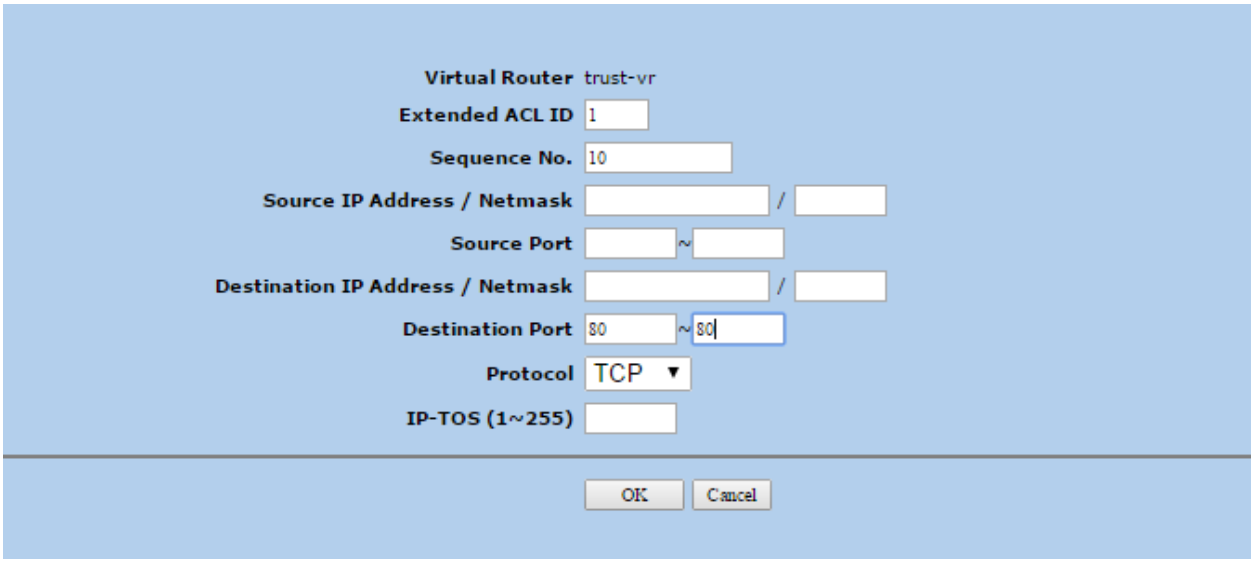
This screenshot shows an action group named WGCSBypass that when combined with a match group in a policy allows specified traffic to bypass McAfee WGCS.



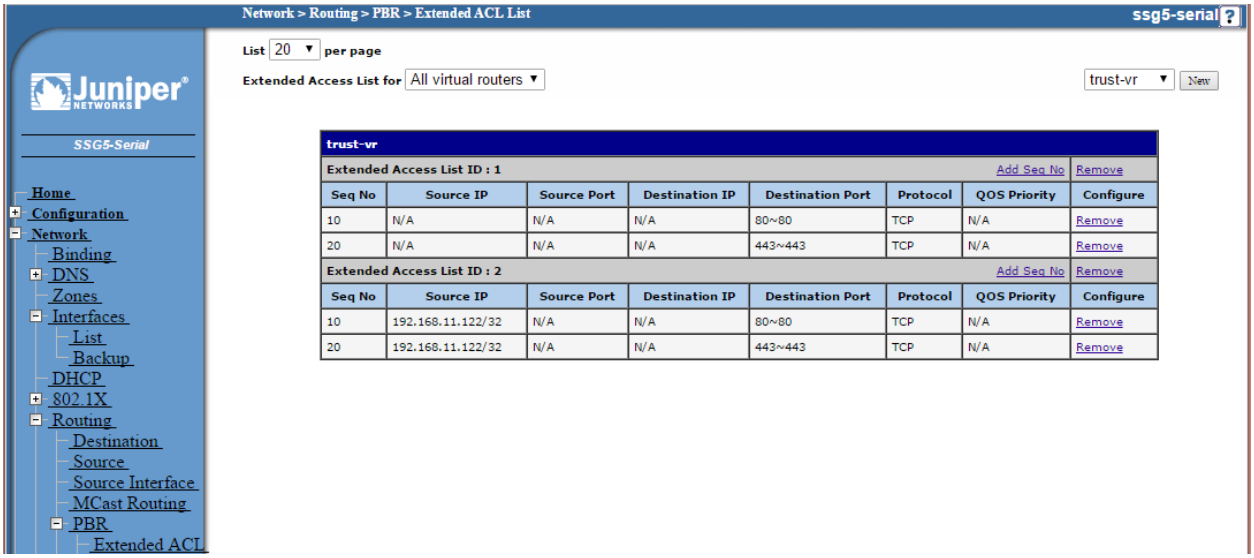
Create an ACL with two entries – When you repeat this procedure for the second entry, use 20 for the sequence number and 443 for the destination port.

From **Network > Routing > PBR > Extended ACL**, configure these settings.

- **Virtual Router** – trust-vr
- **Extended ACL ID** – 1
- **Sequence No.** – 10
- **Destination Port** – 80~80
- **Protocol** – TCP

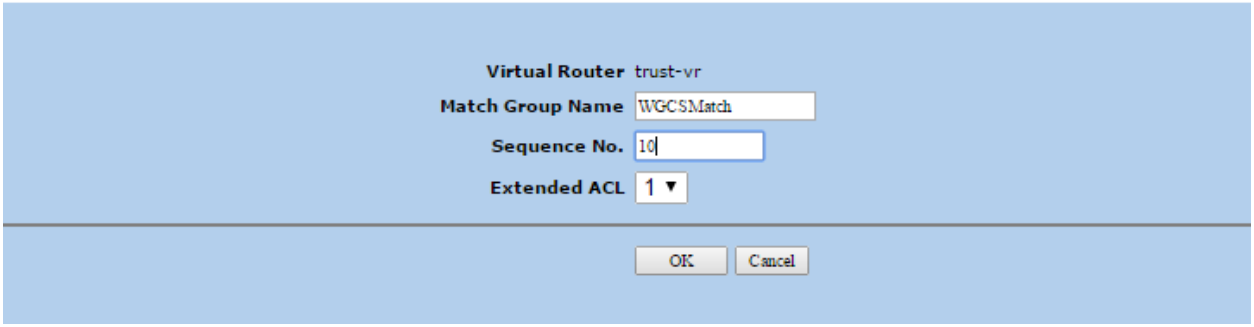


This screenshot shows that ACL 2 that will allow HTTP/HTTPS traffic from the specified source IP address to bypass McAfee WGCS when used in a match group combined with the WGCSBypass action.

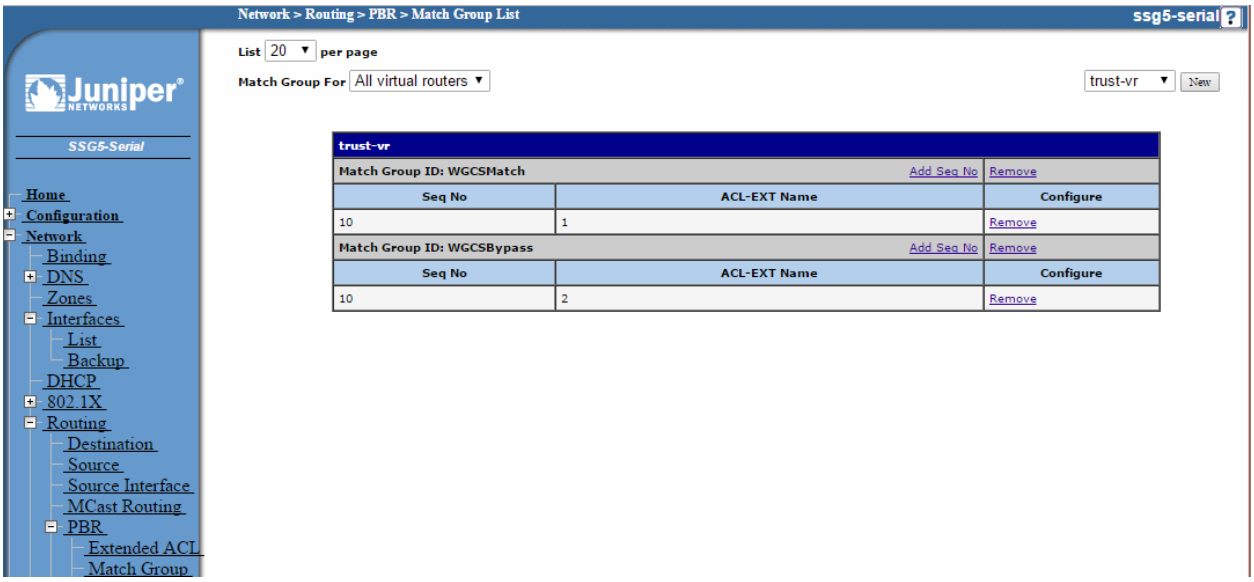


Create a Match Group – Match groups allow you to associate one or more ACLs with a match group name and ID number.

From **Network > Routing > PBR > Match Group**, configure the settings shown in the screenshot.

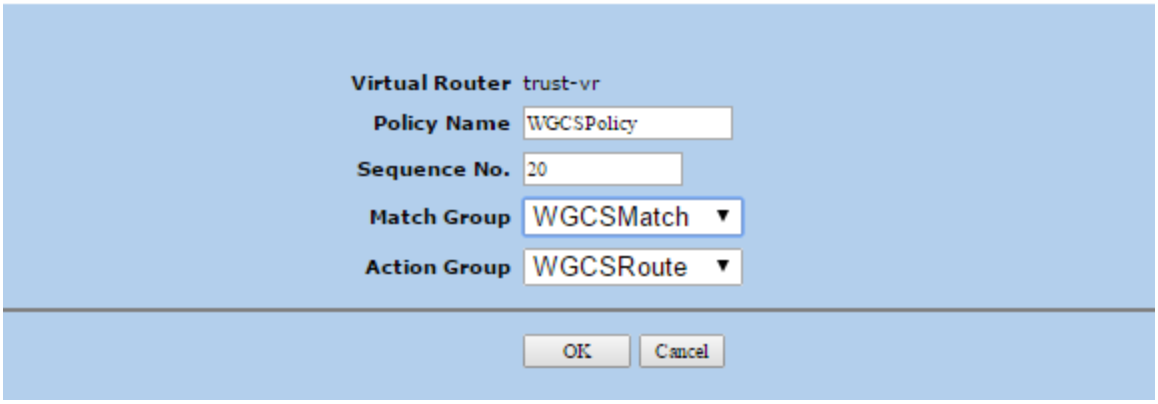


This screenshot shows that ACL 2 is associated with the match group name WGCSBypass. Specify this match group when configuring the policy.

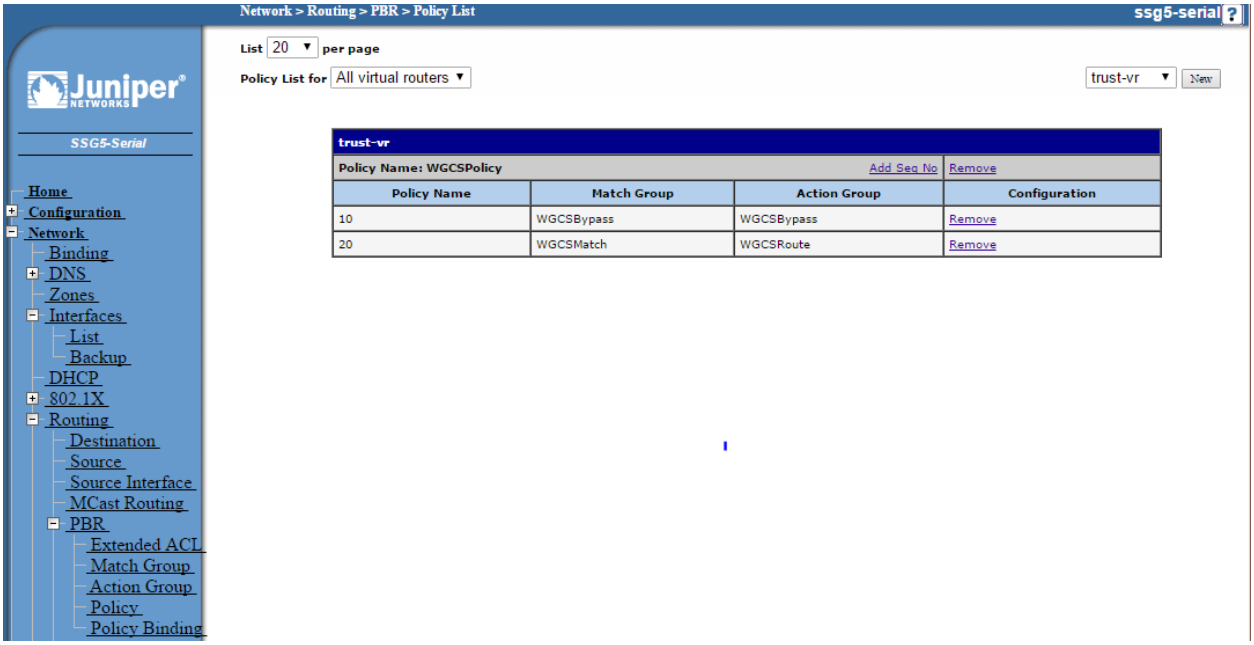


Create a Routing Policy for McAfee WGCS – Policies bind match groups and action groups together.

From **Network > Routing > PBR > Policy**, configure the settings shown in the screenshot.



This screenshot shows the WGCSBypass match and action groups combined in sequence number 10 of the policy named WGCSPolicy. This policy allows the HTTP/HTTPS traffic configured in ACL 2 to bypass McAfee WGCS and go directly to the internet as configured in the WGCSBypass action group.



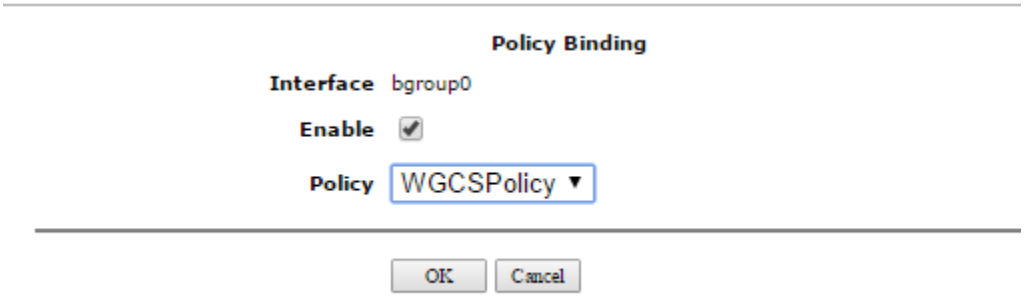
Bind PBR Policy to Client Interface(s)

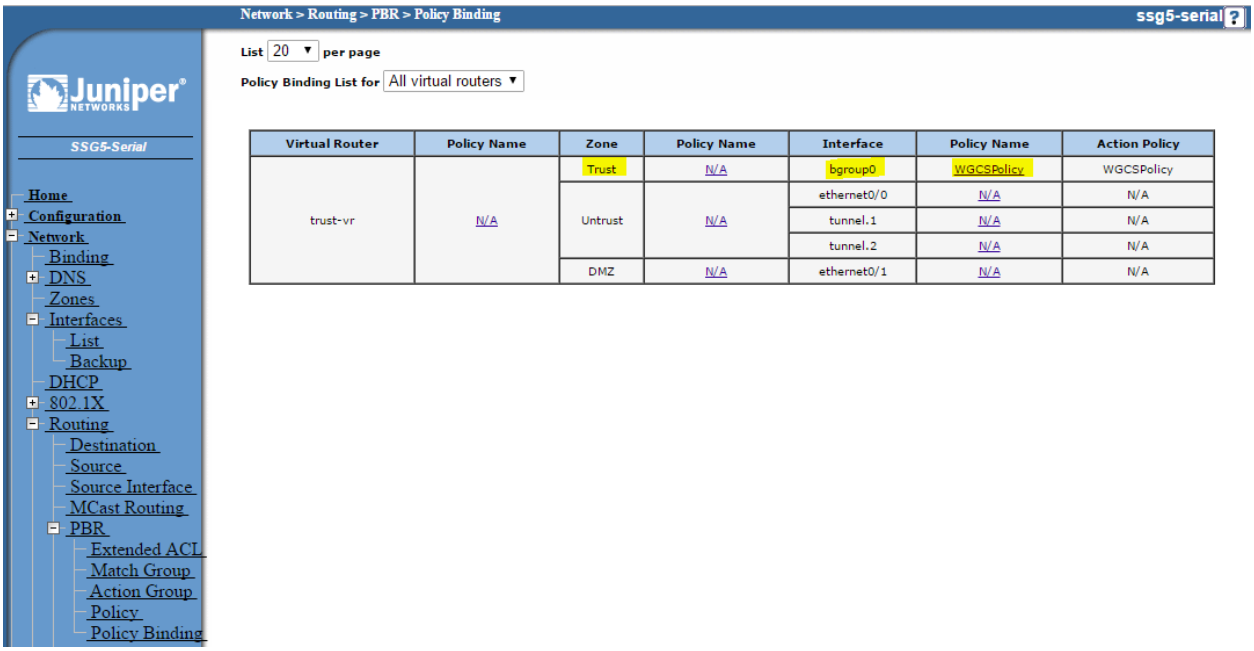
Bind WGCSPolicy to the trusted interfaces.

From **Network > Routing > PBR > Policy Binding**, select the N/A hyperlink under **Policy Name** for the client interface in the Trust zone that you want to edit. Configure these settings.

- **Interface** – bgroup0
- **Enable** – Selected

- **Policy** – WGCSPolicy





Virtual Router	Policy Name	Zone	Policy Name	Interface	Policy Name	Action Policy
trust-vr	N/A	Trust	N/A	bgroup0	WGCSPolicy	WGCSPolicy
		Untrust	N/A	ethernet0/0	N/A	N/A
				tunnel.1	N/A	N/A
				tunnel.2	N/A	N/A
		DMZ	N/A	ethernet0/1	N/A	N/A